



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :

H04L 12/46, G06F 13/00, 15/16

A1

(11) International Publication Number:

WO 92/12587

(43) International Publication Date:

23 July 1992 (23.07.92)

(21) International Application Number: PCT/GB92/00034

(22) International Filing Date: 8 January 1992 (08.01.92)

(30) Priority data:

9100389.7

9 January 1991 (09.01.91)

GB

(71) Applicant: DIGITAL EQUIPMENT CORPORATION
[US/US]; 111 Powdermill Road, Maynard, MA
01754-1499 (US).(71)(72) Applicant and Inventor: HARPER, John [GB/GB]; 3
Kingswood Court, Southcote Road, Reading RG3 2AN
(GB).(72) Inventors: PERLMAN, Radia, J. ; 10 Huckleberry Lane,
Acton, MA 01720 (US). HAWE, William ; 16 Independence
Road, Pepperell, MA 01463 (US).(74) Agent: GOODMAN, Christopher; Eric Potter & Clark-
son, St. Mary's Court, St. Mary's Gate, Nottingham
NG1 1LE (GB).(81) Designated States: AT (European patent), BE (European
patent), CA, CH (European patent), DE (European pa-
tent), DK (European patent), ES (European patent), FR
(European patent), GB (European patent), GR (Euro-
pean patent), IT (European patent), JP, LU (European
patent), MC (European patent), NL (European patent),
SE (European patent).

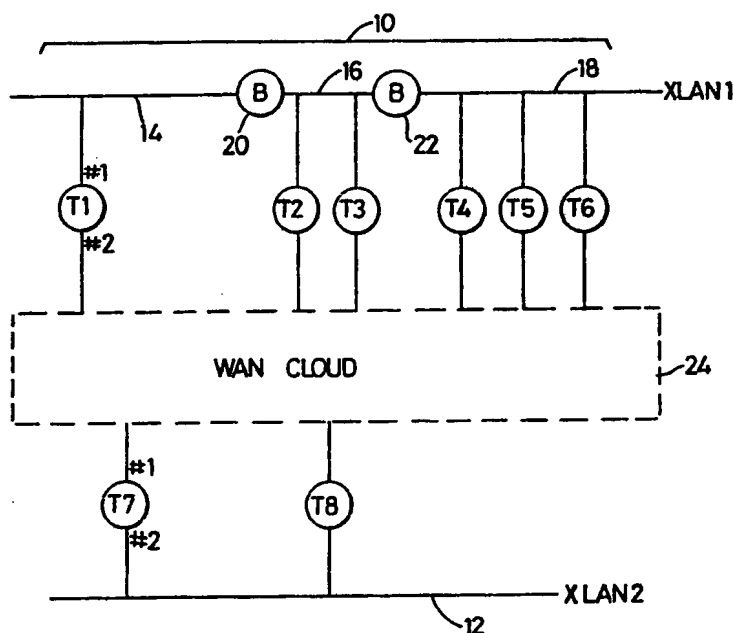
Published

With international search report.

(54) Title: METHOD AND APPARATUS FOR TRANSPARENTLY BRIDGING TRAFFIC ACROSS WIDE AREA NE-
TWORKS

(57) Abstract

A technique for logically connecting local area networks (LANs) that may be separated by wide area networks containing routers and other network components. A logical link is formed between two bridge-like devices called tunnelers, such that, once a tunnel has been established between two LANs, other devices on the LANs can communicate as if the tunnel were a bridge. The tunneling mechanism of the invention requires that each LAN or extended LAN have only one active tunneler at any particular time, referred to as the designated tunneler, and each of the tunnelers is configured to have knowledge of the identities of the other tunnelers. A tunnel is established after a successful exchange of messages between two tunnelers, and then traffic may be forwarded through the tunnel in a transparent manner. The tunneling mechanism permits messages to be forwarded between LANs separated by a wide area network containing routers. Moreover, the mechanism permits filtering of traffic, such that only selected types of traffic, or messages for selected destinations or from selected sources, are forwarded through tunnels. The tunneling mechanism inherently precludes the formation of closed communication loops. An alternate embodiment of the invention optimizes the configuration process for particular network topologies.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland	KR	Republic of Korea	SE	Sweden
CI	Côte d'Ivoire	LI	Liechtenstein	SN	Senegal
CM	Cameroon	LK	Sri Lanka	SU	Soviet Union
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
DE	Germany	MC	Monaco	TG	Togo
DK	Denmark			US	United States of America

METHOD AND APPARATUS FOR TRANSPARENTLY
BRIDGING TRAFFIC ACROSS WIDE AREA NETWORKS

BACKGROUND OF THE INVENTION

5

This invention relates generally to interconnected networks of computers and related devices and, more particularly, to techniques facilitating communication between stations connected to widely separated local area networks (LANs). A local area network includes a set of stations or nodes connected to a common communication bus or ring. Typically, all elements of a single LAN are located in a single building or group of buildings. Multiple LANs are often connected together by devices called bridges, to form an extended LAN. A bridge is a device that is connected to more than one LAN, "listens" to message traffic on each of its LANs, and forwards the traffic onto selected other LANs. The bridge message forwarding operation is limited by a spanning tree algorithm in which all bridges participate. Messages are forwarded only over a loop-free spanning tree, to avoid closed loops and multiple copies of messages. Message forwarding is further controlled by the bridge's "learning" function. Each bridge learns the directional locations of various stations that are the sources of messages it hears, and "remembers" these locations for future use in forwarding message traffic.

Multiple LANs and extended LANs may also be interconnected to form wide area networks (WANs). The mechanism through which extended LANs are interconnected is typically through devices such as routers. At a broad conceptual level, routers perform a similar task to bridges in that each router is connected to multiple LANs or extended LANs. However, the router operates at a different protocol layer (known as the network lay-

er), and a router can be used for forwarding traffic only if the source of the traffic cooperates by using a network layer protocol that is understood by the router. A bridge, on the other hand, is a packet switch that is "transparent." A station that does not have a network layer protocol, or has a network layer protocol that is not implemented by the router, can use the bridge as a packet switch. Unfortunately, however, bridges have significant drawbacks that preclude their use in many contexts.

The most significant drawback of a bridge, as compared with a router, is that bridges use only a subset of the actual topology of the interconnected networks. In particular, redundant paths cannot be used, because to do so would result in closed loops and unwanted multiplication of message traffic. As already mentioned, to ensure a loop-free topology bridges participate in a spanning tree algorithm, which establishes a loop-free tree structure. If two extended LANs were to be interconnected by a bridge, the separate spanning trees of the two networks would have to be combined, forming one larger extended LAN. This might not be desirable from a network administration standpoint. Another important disadvantage of bridges is that they cannot forward traffic through a router, because the packets handled by the bridge do not necessarily have the appropriate network layer information needed to utilize the router. Also, since routers do not participate in the spanning tree algorithm, there is a possibility of forming loops in the topology if bridges were to forward traffic through routers.

In summary, neither routers nor bridges provide an ideal solution to the problems of forwarding message traffic over wide-area networks. Some communication protocols cannot work through routers, since rout-

ers support only certain network layer protocols. But bridges are limited, by the spanning tree algorithm, to a subset of the overall network topology, and cannot be used to forward traffic through routers that separate
5 LANs. Application Serial No. 07/489,910, filed March 7, 1990, entitled "Utilization of Redundant Links in Bridged Networks" (which is owned by the assignee of the present application and identified by docket number PD90-0097), provides for the establishment of point-to-
10 point links outside the spanning tree, but still does not permit forwarding of traffic through traditional routers.

What is needed is a new approach that permits traffic to be forwarded transparently across WANs, using more optimal routes and permitting the traffic to
15 traverse traditional routers. The present invention satisfies this need.

Another way of viewing the problem that this invention solves is that, ideally, there should be some
20 way to address messages directly to particular extended LANs. However, the addressing conventions that have evolved for interconnected networks do not include any convenient means for addressing extended LANs. What is needed, then is some way of forwarding a message more
25 directly to the extended LAN in which the message destination is located. The present invention also satisfies this need.

30

35

SUMMARY OF THE INVENTION

The present invention resides in a method and apparatus for logically interconnecting local area networks and extended local area networks, even if they are separated by wide area networks having traditional routers.

Briefly, the method of the invention includes the steps of providing a number of bridges with the capability to form "tunnels" between LANs that may be widely separated, these special bridges being referred to as tunnelers; then electing a unique designated tunneler for each extended LAN (XLAN) for which tunneling is to be provided. Each XLAN has no more than one designated tunneler, but a single tunneler may be designated by more than one XLAN. The next steps are configuring the tunnelers, by supplying each with information identifying other tunnelers with which a tunnel may be established, establishing at least one tunnel between two designated tunnelers by exchanging messages between the two tunnelers, if the configuration rules state that such a tunnel should exist, and then selectively forwarding message traffic through the established tunnel, from one LAN to another.

In a preferred embodiment of the invention, the step of electing a unique designated tunneler for each XLAN includes executing a spanning tree algorithm among all of the bridges connected to the XLAN, thereby electing a root bridge. Since not all bridges will necessarily have tunnel capability, some adjustment may be needed to bridge priorities used in the spanning tree algorithm, to ensure that the root bridge does have tunneling capability. In this way, the election of a designated tunneler is conveniently effected by means of the existing spanning tree algorithm.

The step of configuring the tunnelers includes supplying to each tunneler the identities of other tunnelers and the identities of ports through which the other tunnelers are connected to XLANS with which the ports are associated. The step of establishing a tunnel includes transmitting a greeting from a designated tunneler to each other tunneler that is a potential tunnel endpoint, receiving a message from one of the potential tunnel endpoints confirming that a tunnel may be established, and recording the successful establishment of a tunnel. Establishing a tunnel may also include the steps of transmitting a greeting to at least one backup tunneler, after failing to receive a confirming message from the other designated tunneler; then receiving a message from the backup tunneler confirming that a tunnel may be established; and finally recording the successful establishment of the tunnel.

The step of selectively forwarding message traffic through the established tunnel includes the steps of receiving a message at a tunneler, and determining whether the message destination is known to the tunneler. If the destination is known, the method further includes the steps of determining whether a tunnel is required to reach this particular destination, and, if so, forwarding the message through the tunnel, if the tunnel has been established and the message is of a type authorized for forwarding through the tunnel.

If the destination is not known, a subsequent step in the method is determining whether the message was received from a tunnel. If so, the message is forwarded through a port defined as the tunnel endpoint. If the message was not received from a tunnel and the message destination is not known, the method further includes forwarding the message over all non-tunnel ports in the spanning tree, except the one through

client transmit
a greeting ⇒

transmit
greeting
to backup
tunnel

fail to
receive
message

destination
is not
known

which the message was received, and forwarding the message through all established tunnels, if any, for which this tunneler is a sending endpoint, if the message is of a type authorized for transmission through the tunnel.

Forwarding a message through a tunnel includes the step of appending to the message a destination address comprising the address of a receiving endpoint tunneler of the tunnel, and a port identifier that also defines, in part, the receiving endpoint of the tunnel. Then the message is transmitted through an appropriate port to reach the receiving endpoint of the tunnel. If the message was received from a tunnel, the method further comprises the step of stripping the tunnel receiving endpoint address from the received message, before forwarding it through the tunnel receiving endpoint port.

In an alternate embodiment of the invention, the configuring step is optimized for specific network topologies. In this case the step of configuring includes supplying the tunnelers with a subset of information concerning other tunnelers, the subset of information being optimized for a particular network topology. The step of establishing a tunnel then includes one or more of the following steps:

(1) For a designated tunneler, sending a greeting to another designated tunneler with which it has been configured, and receiving a response confirming that a tunnel has been established;

(2) for a designated tunneler, sending a greeting to a nondesignated tunneler with which it has been configured, receiving a refusal response identifying a designated tunneler, redirecting the greeting to the designated tunneler identified in the refusal response, and receiving a response confirming that a tunnel has been established; and

← refusal response

(3) for a nondesignated tunneler, periodically transmitting multicast messages identifying the tunnelers with which it has been configured, and, for a designated tunneler, responding to a multicast message from
5 a nondesignated tunneler, by sending a greeting to one of the tunnelers contained in the multicast message, and receiving a response message confirming that a tunnel has been established.

The optimized configuration approach reduces
10 the burden of having to manually configure every tunnel-
er with knowledge of every other tunneler. The cost of
this simplification is some added complexity in the es-
tablishment of tunnels, but the approach is worthwhile
for some network topologies.

15 It will be understood that the invention also
encompasses equivalent apparatus claims similar in
scope to the various forms of the method discussed
above.

It will be appreciated from the foregoing that
20 the present invention represents a significant advance
in the field of communication networks. In particular,
the invention provides a novel way of logically inter-
connecting two LANs, even through they may be separated
by wide area networks containing routers. The tunneling
25 protocol of the invention effects this logical intercon-
nection in a manner that permits user controlled filter-
ing of the tunnel traffic, and precludes the formation
of any closed loops. Traffic filtering may fulfill any
desired network administration objectives, such as
30 limiting traffic flow through a tunnel to selected
protocols, or limiting flow through a tunnel to traffic
having selected destination or source addresses. Other
aspects and advantages of the invention will become
apparent from the following more detailed description,
35 taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a simplified schematic diagram of one example of a network topology having multiple extended local area networks (XLANS) that are connected through a wide area network (WAN) having conventional routers;

FIG. 2 is a diagram similar to FIG. 1, but showing a different topology example;

FIG. 3 is a diagram similar to FIG. 1, but showing yet another topology example;

FIG. 4 is a flowchart depicting the operations performed in establishing tunnels;

FIG. 5 is a flowchart depicting the operations performed by a tunneler in processing and forwarding received messages; and

FIG. 6 is diagram similar to FIGS. 1-3, but showing another topology, in which a configuration optimization is employed.

20

25

30

35

DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in the drawings by way of illustration, the present invention is concerned with a novel
5 technique for logically interconnecting multiple local
area networks (LANs) or extended local area networks
(XLANS), which may be separated by wide area networks
(WANs) containing traditional routers. Neither routers
nor bridges can perform this function in all situa-
10 tions, since routers do not support all communications
protocols, and bridges are limited by the spanning tree
algorithm and cannot forward traffic through tradition-
al routers.

In accordance with the invention, each LAN or
15 XLAN has a bridge-like device that is designated as the
"tunnelers" for that network, and logical connections,
called tunnels, are established between pairs of tunnel-
ers. Each such pair of tunnelers functions in much the
same way as bridge, in the sense that traffic is for-
20 warding transparently from one network to another. Each
tunnelers has a connection to the LAN or XLAN of which
it is the designated tunnelers, and at least one connec-
tion to a WAN that separates the LANs or XLANS.

FIG. 1 is one example, in simplified form, of
25 a network topology in which the invention may be used.
The topology includes two extended LANs 10, 12, indicat-
ed as XLAN1 and XLAN2. XLAN1 has three LANs 14, 16, 18
connected by bridges B, indicated at 20, 22. XLAN2 12
is a single LAN. The rest of the topology is a WAN 24,
30 referred to as a "WAN cloud." This includes any combina-
tion of LANs, point-to-point links, bridges, and rout-
ers. The WAN cloud 24 handles message traffic in accor-
dance with conventional routing protocols, for instance
(but not restricted to) the Open Systems Interconnec-
35 tion (OSI) Reference Model, developed by the Inter-

national Standards Organization (ISO). The problem with which the invention is concerned is how to establish a communication link between XLAN1 and XLAN2, such that traffic can be forwarded through the WAN cloud 24, as
5 optimally as possible, even if the source or destination of the traffic is not operating in accordance with the routing protocols in the WAN cloud. In this illustration, XLAN1 is connected to the WAN cloud 24 by six "tunnelers" indicated as T1, T2, T3, T4, T5, and T6,
10 and XLAN2 is connected to the WAN cloud by two tunnelers T7 and T8. Tunneler T1 is connected to LAN 14, tunnelers T2 and T3 are connected to LAN 16, and tunnelers T4, T5 and T6 are connected to LAN 18. Each tunneler may considered as performing in some ways like a
15 bridge, but having additional tunneling capability, to be described in detail below.

The tunneling capability involves a preliminary procedure for establishing tunnels, and then a traffic handling procedure whereby traffic may be forwarded through the established tunnels. Establishing
20 the tunnels is effected by two basic steps. First, a procedure is used to ensure that there is only one designated tunneler for each LAN or extended LAN under consideration. Second, the designated tunnelers are manually "configured" by an operator or network manager, to
25 define the tunnels that can be established for each pair of LANs or extended LANs.

Although each LAN or extended LAN has only one designated tunneler, the same tunneler may perform the
30 function of designated tunneler for more than one LAN or extended LAN. This point is not clear from FIG. 1 but will become apparent from a later example.

There are two alternatives for ensuring that each LAN or XLAN has only one designated tunneler. The
35 first alternative, and probably the easiest to imple-

ment, is to use the same procedure that the spanning tree algorithm uses to elect a root bridge. In the spanning tree algorithm, a single bridge is elected and designated the "root bridge" for each extended LAN, to ensure that interconnected bridges in the extended LAN form a loop-free topology. If the same procedure is used to elect a tunneler, it must be used in such a way as to ensure that the elected bridge has tunneling capability. If only some of the bridges participating in the spanning tree algorithm have tunneling capability, some adjustment would need to be made to bridge priorities used in the spanning tree algorithm, to ensure that the bridge elected as the root bridge also has tunneling capability. Using the spanning tree algorithm to elect a designated tunneler has the advantage that the procedure already exists and is utilized by bridges in the network. Moreover, the spanning tree algorithm operates effectively even in periods of heavy traffic congestion.

The alternative to using an existing spanning tree algorithm to designate a tunneler is to implement a special election process among the potential tunnelers in each extended LAN. This algorithm could be closely duplicative of the spanning tree algorithm, wherein each tunneler transmits a previously assigned priority, and a collective election process eliminates all but one of the tunnelers. This has some disadvantages associated with the implementation of a special election procedure, principally additional cost and complexity. Moreover, there is no guarantee that such a procedure would work effectively in heavy traffic conditions. Since multicast messages look like ordinary data packets, and compete with other data packets for access to the network, election messages may be discarded under some conditions.

The other preliminary task is to configure, by network management, the tunnelers with the definitions of tunnels that should be built. For example, in FIG. 1, if the designated tunneler for XLAN1 is T1 and the designated tunneler for XLAN2 is T7, the tunnel between XLAN1 and XLAN2 would be defined by the network layer address of each end-point of the tunnel and by the port through which the end-point is connected to the appropriate XLAN. If T1 is connected to XLAN1 by its #1 port, and T7 is connected to XLAN2 by its #2 port, the complete definition of the tunnel is (T1,1), (T7,7). Tunneler T1 is configured with a corresponding tunnel definition as seen from the T1 end, i.e. (1,T7,2). Tunneler T7 is configured with a tunnel definition as seen from the T7 end, i.e. (2,T1,1).

Configuration optionally involves two other types of information. First, alternate tunnel definitions may be configured into the tunnelers. For example, T1 may be configured to use T8 as an alternate tunnel end-point, in the event that T7 is not available for some reason. The second type of additional configuration data includes a definition of the types of messages that will be forwarded over each tunnel. The tunnel may be used for only selected protocols, or for all types of traffic, or for traffic involving only selected destinations or sources, all at the option of the network manager.

After election of a designated tunneler for each LAN or extended LAN, and configuration of the designated tunnelers, tunnels are established by an exchange of messages between tunnelers that have been defined as tunnel end-points. For example, T1, having been configured to establish a tunnel to T7, will send a greeting message through the WAN cloud 24, addressed to T7. In essence, the greeting indicates that T1

wishes to establish a tunnel with T7. T7 sends a reply message, either assenting to the establishment of a tunnel, or indicating that it (T7) is not the designated tunneler for the requested port, or indicating that it
5 (T7) has not been configured for this tunnel. Another possibility is that T7 cannot be reached for some reason, and no reply is received by T1. This exchange may take place in the opposite direction, depending on timing considerations. Or there may be a symmetrical
10 exchange, with both tunnelers sending messages to their opposite numbers in the defined tunnel.

After a tunnel is established, such as the tunnel T1-T7, it functions in a similar fashion to a bridge connecting the two XLANs. When tunneler T1
15 "hears" a message on XLAN1, T1 forwards the message through the tunnel to tunneler T7, after first appending the network layer address for T7. On receiving such a message, tunneler T7 strips off the network layer address and forwards the message onto XLAN2. Traffic may
20 also be transmitted through the tunnel in the opposite direction by the same mechanism.

The tunnelers have a bridge-like capability of learning the locations of stations from which messages have come. Each message has a source address, in the
25 form of a data link layer address. When tunneler T1, for example, receives traffic through its #1 port, this traffic can be identified as having a source address in the direction of XLAN1. A subsequent message having a destination address that corresponds with a source
30 address previously noted as emanating from XLAN1, need not be forwarded through the tunnel to T7. However, when the direction of a destination address is not known to the tunneler, the message is forwarded through the established tunnel to XLAN2.

35 FIG. 2 depicts another example of a topology,

having a WAN cloud 24, two tunnelers T1 and T2, and a total of eight extended LANs, indicated as XLAN1 through XLAN8. XLAN1 through XLAN5 are connected to tunneler T1 through its ports #1 through #5, and XLAN6 through XLAN8 are connected to tunneler T2 through its ports #1 through #3. Tunneler T1 is connected through its additional port #6 to the WAN cloud 24 and tunneler T2 is connected to the WAN cloud through its additional port #4. T1 is the designated tunneler for extended LANs XLAN1 through XLAN5, and T2 is the designated tunneler for extended LANs XLAN6 through XLAN8. Tunnelers T1 and T2 may be configured to establish as many as fifteen tunnels between various pairs of XLANs connected to different tunnelers. For example, the tunnels from XLAN1 will be configured as:

(1,T2,1), for tunneling from XLAN1 to XLAN6,
(1,T2,2), for tunneling from XLAN1 to XLAN7,
and (1,T2,3), for tunneling from XLAN1 to XLAN8.

Four additional sets of three tunnels can be configured with XLAN2 through XLAN5 as the starting points. Additional tunnels may be established between pairs of XLANs connected to the same tunneler, such as XLAN4 and XLAN5. There are ten possible additional tunnels using only T1 for both tunnel endpoints, and three possible additional tunnels using T2 for both tunnel endpoints. Although XLAN4 and XLAN5, for example, can be connected using T1 as a conventional bridge, a tunnel may be a more desirable solution because it provides a convenient mechanism for filtering traffic between the two XLANs. Moreover, if the two XLANs are conventionally bridged by T1, their spanning trees will necessarily have to be merged and this may not be desirable.

For purposes of illustration, the WAN cloud 24 in FIGS. 1 and 2 has been shown as being separate from the other extended LANs in the topology. In general,

however, the principles of the invention discussed above also apply if the cloud is considered to encompass the extended LANs between which the tunnels are established.

5 The requirement that there be only one designated tunneler for each extended LAN leads to a desirable, and not immediately obvious property of networks connected by tunnels. When tunnels are established in accordance with the invention, there is no possibility
10 of closed loops being formed by any interconnection of the tunnels. This property can be understood from the further example of FIG. 3, which shows a topology including four extended LANs, XLAN1 through XLAN4, each of which has a designated tunneler T1 through T4, respectively. The established tunnels include T1-T2,
15 T2-T3, T3-T4 and T4-T1, which form the sides of square, together with T1-T3 and T2-T4, which form the diagonals of the square. At first sight, it might appear that a message could be circulated around the sides of the
20 square in a closed loop, and that unwanted duplicate messages would be generated.

 Suppose a message from XLAN1 is to be forwarded by tunneler T1, and that the destination is unknown to T1. T1 will forward the message over its three established tunnels. T1-T2, T1-T3 and T1-T4. If, for example,
25 the message destination is on XLAN3, it will be forwarded there via tunnel T1-T3. Tunneler T2 will also receive a copy of the message, through tunnel T1-T2, but will not forward the message through a second tunnel, such as T2-T3. There is only one established
30 tunnel between T1 and T3, and that is the "diagonal" tunnel T1-T3. Each tunneler is conditioned to operate such that traffic received through one tunnel should not be forwarded through another. Since there is only
35 one designated tunneler for each extended LAN, this

rule is simple to put into effect.

The procedure performed by each tunneler in establishing tunnels is shown in simplified flowchart form in FIG. 4. The tunneler first determines if it is
5 the uniquely designated tunneler for a particular extended LAN (XLAN), as indicated in block 30, and then determines whether this tunneler has been configured as a tunneler to another XLAN, as indicated in block 32. If the answer to either of these questions is negative,
10 the tunneler shifts its attention to other XLANs to which it may be connected (block 34) and repeats the questions of blocks 30 and 32. If the tunneler is a designated tunneler for a particular XLAN and has been configured as a tunneler to some other XLAN, the next step
15 is to perform a communications "handshake" with the tunneler that has been configured as the other endpoint of the tunnel. The handshake, indicated in block 36 may take any of several forms, but two possible results of the handshake are that the establishment of tunnel is
20 confirmed, as indicated by line 38 from block 36, or that the establishment of the tunnel is refused for some reason, as indicated by line 40. In the latter case, there may be subsequent communication with an alternate tunnel endpoint, if one has been specified by
25 configuration, as indicated in block 42. In any event, after establishment of a tunnel has been confirmed or refused, the tunneler repeats this entire process for other XLANs to which it may connected, as indicated in block 34.

30 The operations performed by a tunneler in forwarding messages are summarized in FIG. 5. Like a bridge, a tunneler has multiple ports that are connected to separate LANs or XLANs. In addition to its physical ports, a tunneler may be considered to have a "tunnel
35 neler port" for each established tunnel for which the

tunnelers serve as end-points. When a message is received at a tunneler, as indicated at 50, the source address of the message is noted, in conjunction with the port from which the message was received, and a
5 database of addresses and their port locations is developed. This learning function, indicated in block 52, includes learning the locations of addresses in terms of their corresponding "tunnel ports" of the tunnelers.

If the destination of the received message is
10 known from prior message activity, as determined in block 54, the identity of the port through which the message should be forwarded is already known, and the message may be forwarded, as indicated in block 56. The destination may, for example, be located on a LAN that
15 is directly connected to the tunnelers, in which case the message can be forwarded through the appropriate non-tunnel port. If the known destination may be reached through an established tunnel, and if the message is of a type that has been authorized for forwarding
20 through a tunnel, then the message is forwarded through the established tunnel. This requires that a network layer address be appended to the message, giving the address of the receiving end-point of the tunnel. Then the message is forwarded through the
25 tunnel.

If the destination of the received message is not known, the tunnelers next determine whether the message was received from a tunnel, as indicated in block 58. If so, the message is simply forwarded through the
30 appropriate port that has been designated as the tunnel receiving end-point, as indicated in block 60. The message, having been received from a tunnel, is not forwarded through any other tunnels, and the possibility of closed loops is avoided. If the received message was
35 not received from a tunnel, and its destination is un-

known, it should be forwarded through all non-tunnel ports permitted by the spanning tree, and through all tunnel ports, i.e. through all tunnels for which the tunneler is functioning as an end-point, as indicated
5 in block 62. In forwarding through the tunnel ports, the tunneler must first check that the tunnels have been established and that the message is of a type authorized for forwarding through tunnels.

The foregoing description is not intended to
10 preclude the possibility of a tunnel being established between two extended LANs connected to the same tunnel-er, i.e. where one tunneler is used as both endpoints of a tunnel, but using different ports, of course . Although this type of interconnection could be handled by
15 the conventional bridge function, the tunnel mechanism provides the additional capability of filtering traffic in some desired way, such that only certain categories will be allowed to pass through the tunnel. Also, as noted earlier, using the tunneling mechanism avoids
20 having to merge the spanning trees of the two bridged networks.

The tunneling mechanism described above works to advantage in any of a variety of network configurations. In particular, the use of tunnels in accordance
25 with the invention allows traffic to be bridged from one extended LAN to another, even when an interposed WAN includes routers. Considered from another perspective, the invention provides a means for addressing extended LANs. Conventional communications protocols provide no means for addressing LANs and extended LANs,
30 but the invention achieves this objective since a designated tunneler and an associated port are unique to a LAN or extended LAN. Thus the tunneler-port identification also identifies the LAN. Moreover, tunneling is
35 achieved by a mechanism that precludes the formation of

undesirable closed loops, allows grouping of tunnelers to designate alternates, and can make use of an existing spanning tree algorithm to elect a designated tunneler for each extended LAN.

5 Tunnel configuration, in accordance with the invention as described thus far, requires each potential tunneler to be configured with a knowledge of all of the other potential tunnelers. For example, in the topology of FIG. 1, each of the six tunnelers connected
10 to XLAN1 has to be configured with knowledge of the two tunnelers connected to XLAN2 and each of the two tunnelers connected to XLAN2 has to be configured with knowledge of all six of the tunnelers connected to XLAN1. In total there will be 2×6 pieces of configuration
15 information for the FIG. 1 topology. In an alternate embodiment of the invention, the amount of configuration information can be reduced, or optimized, based on knowledge of the specific network topology in which the invention is being used. An example of a topology in
20 which such an optimization scheme could be used is shown in FIG. 6.

FIG. 6 shows four extended LANs, designated XLAN1, XLAN2, XLAN3 and XLAN4. XLAN1 is connected to a tunneler T1, which is connected to another tunneler T2
25 through a point-to-point link L1. The tunneler T2 is connected by another port to XLAN4. Similarly, XLAN2 is connected to XLAN4 through a path comprising tunneler T4, link L2, and tunneler T3. Finally, XLAN3 is connected to XLAN4 through a path comprising tunneler T5, link
30 L3, and tunneler T6. The links L1, L2, L3, may be considered a special case of the WAN shown in FIG. 1. In the configuration of FIG. 6, it is further assumed that there is a desire to build tunnels from XLAN4 to each of the other extended LANs, XLAN1, XLAN2 and XLAN3.

35 In accordance with this embodiment of the

invention, every tunneler does not have to be configured with information concerning every other possible tunneler. For example, in the network configuration of FIG. 6 it would only be necessary to configure a tunnel
5 between T1 and T2 (for XLAN1-XLAN4), another tunnel between T3 and T4 (for XLAN2-XLAN4), and another tunnel between T5 and T6 (for XLAN3-XLAN4). There is no point in configuring T1 with knowledge of T3 and T6, because
10 T2 is inoperative. Of course, this arrangement using three tunnelers connected with XLAN4 is inconsistent with the notion that there is only one tunneler for each XLAN.

In this optimization approach of the invention,
15 tion, there are three possible ways that a tunneler would know whether to build a tunnel. The first is the manual configuration technique as described for the basic form of the invention. Thus, if T2 were the designated tunneler for XLAN4, the tunnel from T1 to T2
20 would be established as a result of this basic manual configuration technique. The second technique is by multicast advertisement, and the third is by redirection, both of which need further explanation.

A multicast message is one directed to multiple destinations. In the second technique for establishing tunnels, if a tunneler is not elected the designated tunneler for a particular XLAN, it periodically multicasts the set of tunnels with which it has been manually configured. Thus, T3, which is not the
30 designated tunneler, would advertise by multicast messages that it had been configured to form a tunnel with T4. The designated tunneler T2, upon hearing of the advertised T3-T4 tunnel from T3's multicast, establishes a second tunnel, between T2 and T4. This
35 would certainly not be an optimally routed tunnel. A

message from XLAN4 bound for XLAN2 would proceed to tunneler T2, which would forward the message to the other tunnel endpoint, T4, but through XLAN4 and T3. Similarly, tunneler T6 would advertise a tunnel from T6 to T5, with which it had been configured, and the designated tunneler would receive T6's multicast advertisement and establish a tunnel from T2 to T5.

Tunnel establishment by redirection occurs when a tunneler attempts communication with a tunneler that has not been elected the designated tunneler. The return message from the non-designated tunneler includes the identity of the designated tunneler, so the tunneler attempting communication is made aware which tunneler, and which of its ports on that XLAN, will accept the tunnel request. A simple protocol is provided, to require the designated tunneler to advertise its identity, including a port number, to others on the same XLAN. For example, tunneler T5 has been configured to establish a tunnel with T6, but T6 is not the designated tunneler. A response message from T6 redirects T5 to the designated tunneler T2. T6 has knowledge of the designated tunneler T2 from "advertising" messages it has previously received from T2. Similarly, tunneler T3 redirects T4 to the designated tunneler T2. Communication in a direction toward XLAN4 is also non-optimal. For example, a message from XLAN3 over tunnel T5-T2 is constrained to first visit the designated tunneler T2, which is reached through XLAN4, before returning to XLAN4 for delivery to its final destination.

The advantage of optimization by this approach is that the storage and time requirements for manual configuration are greatly reduced. The trade-offs for this improvement are that message routing is likely to be further removed from optimal, and the approach is not universally applicable to all network configurations.

It will be appreciated from the foregoing that the present invention represents a significant advantage in the field of interconnected local area networks (LANs). In particular, the invention permits LANs to be
5 bridged together through an established communications tunnel even when they are separated by network components that include routers. Each tunnel established in accordance with the invention provides for user-specified filtering, wherein traffic flowing through the
10 tunnel may be limited, at the user's option, to specific categories or protocols, or may be limited in other ways, such as by source or destination. As described, the tunnel mechanism of the invention inherently precludes closed loops in the interconnected network. The
15 basic tunneling approach provides for grouping of tunnelers to define alternatives in the event of an inoperative tunnel. In the optimization approach described, manual tunneling configuration is greatly reduced for some network configurations. It will also
20 be appreciated that, although a basic embodiment and a specifically optimized version of the invention have been described in detail for purposes of illustration, various modifications may be made without departing from the spirit and scope of the invention. Accordingly,
25 ly, the invention is not to be limited except as by the appended claims.

30

35

CLAIMSWe claim:

1. A method for logically connecting local area networks (LANs) interconnected by network components that include bridges and may include routers, the method comprising the steps of:

- 5 providing selected bridges with the capability to form tunnels between LANs that may be widely separated, such bridges being referred to as tunnelers;
- electing a unique designated tunneler for each extended LAN (XLAN) for which tunneling is to be provided,
- 10 ed, wherein each XLAN has no more than one designated tunneler, but a single tunneler may be designated by more than one XLAN;
- configuring the tunnelers by supplying each with information identifying other tunnelers with which
- 15 a tunnel may be established;
- establishing at least one tunnel between two designated tunnelers, by exchanging messages between the two tunnelers; and
- selectively forwarding message traffic through
- 20 the established tunnel, from one LAN to another.

2. A method as defined in claim 1, wherein the step of electing a unique designated tunneler for each XLAN includes:

- executing a spanning tree algorithm among all
- 5 of the bridges connected to the XLAN, and thereby electing a root bridge; and
- ensuring that the root bridge has tunneling capability.

3. A method as defined in claim 1, wherein the step of configuring the tunnelers includes:

supplying to each tunneler the identities of other tunnelers and the identities of ports through
5 which the other tunnelers are connected to XLANS with which they are associated.

4. A method as defined in claim 3, wherein the step of establishing at least one tunnel includes:

transmitting a greeting from a designated tunneler to each other tunneler that is a potential tunnel
5 endpoint;

receiving a message from one of the potential tunnel endpoints confirming that a tunnel may be established; and

recording that a tunnel has been established.

5. A method as defined in claim 1, wherein the step of configuring the tunnelers includes:

supplying to each tunneler the identities of other tunnelers, the identities of ports through which
5 the other tunnelers are connected to XLANS with which they are associated, and an indication of tunneler priorities, to facilitate establishment of tunnels between tunnel endpoints.

6. A method as defined in claim 5, wherein the step of establishing at least one tunnel includes:

transmitting a greeting from a designated tunneler to another designated tunneler that is a potential tunnel endpoint;
5

receiving a message from the other designated tunneler confirming that a tunnel may be established; and

recording that a tunnel has been established.

7. A method as defined in claim 5, wherein the step of establishing at least one tunnel includes:

transmitting a greeting from a designated tunnel-
neler to another designated tunnel-er that is a poten-
5 tial tunnel endpoint;

transmitting, after failing to receive a con-
firming message from the other designated tunnel-er, a
greeting to at least one backup tunnel-er;

receiving a message from the backup tunnel-er
10 confirming that a tunnel may be established; and
recording that a tunnel has been established.

8. A method as defined in claim 1, wherein the step of selectively forwarding message traffic through the established tunnel includes:

receiving a message at a tunnel-er;
5 determining whether the message destination is
known to the tunnel-er;

if the destination is known, performing the
steps of

determining whether the destination re-
quires forwarding through a tunnel, and
10

if so, forwarding the message through the
tunnel, if the tunnel has been established and
the message is of a type authorized for for-
warding through the tunnel;

15 if the destination is not known, determining
whether the message was received from a tunnel;

if the message was received from a tunnel, for-
warding the message through a port defined as the tun-
nel endpoint;

20 if the message was not received from a tunnel
and the message destination is not known, performing
the steps of

 forwarding the message over all permissi-
ble non-tunnel ports, and

25 forwarding the message through all estab-
lished tunnels, if any, for which this tunnel-
er is a sending endpoint, if the message of a
type authorized for tunnel transmission.

9. A method as defined in claim 8, wherein the
step of forwarding a message through a tunnel includes:

 appending to the message a destination address
that includes the address of a receiving endpoint tun-
5 neler of the tunnel, and also includes a port identifi-
er that defines, in part, the receiving endpoint of the
tunnel; and

 transmitting the message through an appropri-
ate port to reach the receiving endpoint of the tunnel.

10. A method as defined in claim 9, wherein:

 if the message was received from a tunnel the
method further comprises the step of stripping, from
the received message, the tunnel receiving endpoint ad-
5 dress, before forwarding the message through the tunnel
receiving endpoint port.

11. A method as defined in claim 8, wherein
the step of selectively forwarding messages through a
tunnel includes the further step of:

 updating, if necessary, a database of destina-
5 tions, by means of address information obtained from
each message source.

12. A method as defined in claim 1, wherein:

the step of configuring includes supplying the tunnelers with a subset of information concerning other tunnelers, the subset of information being optimized

5 for a particular network topology; and

the step of establishing a tunnel includes the steps of

(1) for a designated tunneler, sending a greeting to another designated tunneler with which it has been configured, and receiving a response confirming that a tunnel has been established,

10

(2) for a designated tunneler, sending a greeting to a nondesignated tunneler with which it has been configured, receiving a refusal response identifying a designated tunnel-er, redirecting the greeting to the designated tunneler identified in the refusal response, and receiving a response confirming that a tunnel has been established, and

15

20

(3) for a nondesignated tunneler, periodically transmitting multicast messages identifying the tunnelers with which it has been configured, and, for a designated tunneler, responding to a multicast message from a nondesignated tunneler, by sending a greeting to one of the tunnelers contained in the multicast message, and receiving a response message confirming that a tunnel has been established.

25

13. A method for logically connecting local area networks (LANs) interconnected by network components that include bridges and may include routers, the method comprising the steps of:

- 5 providing some of the bridges with the capability to form tunnels between LANs that may be widely separated, such bridges being referred to as tunnelers;
 - electing a unique designated tunneler for each extended LAN (XLAN) for which tunneling is to be provided,
- 10 wherein each XLAN has no more than one designated tunneler, but a single tunneler may be designated by more than one XLAN;
 - configuring the tunnelers by supplying each tunneler with the identities of other tunnelers and the
- 15 identities of ports through which the other tunnelers are connected to XLANs with which they are associated;
 - establishing at least one tunnel between two designated tunnelers, by transmitting a greeting from a designated tunneler to each other tunneler that is a
- 20 potential tunnel endpoint, receiving a message from one of the potential tunnel endpoints confirming that a tunnel may be established, and recording that a tunnel has been established; and
 - selectively forwarding message traffic through
- 25 the established tunnel, from one LAN to another.

14. A method as defined in claim 13, wherein the step of selectively forwarding message traffic through the established tunnel includes:

- receiving a message at a tunneler;
- 5 determining whether the message destination is known to the tunneler;

if the destination is known, performing the steps of

10 determining whether the destination requires forwarding through a tunnel, and

if so, forwarding the message through the tunnel, if the tunnel has been established and the message is of a type authorized for forwarding through the tunnel;

15 if the destination is not known, determining whether the message was received from a tunnel;

if the message was received from a tunnel, forwarding the message through a port defined as the tunnel endpoint;

20 if the message was not received from a tunnel and the message destination is not known, performing the steps of

25 forwarding the message over all non-tunnel ports except one through which the message was received,

forwarding the message through all established tunnels, if any, for which this tunnel-er is a sending endpoint, if the message is of a type authorized for tunnel transmission.

15. A method as defined in claim 14, wherein the step of forwarding a message through a tunnel includes:

5 appending to the message a destination address that includes the address of a receiving endpoint tunnel-er of the tunnel, and also includes a port identifier that defines, in part, the receiving endpoint of the tunnel; and

10 transmitting the message through an appropriate port to reach the receiving endpoint of the tunnel.

16. A method as defined in claim 15, wherein:
if the message was received from a tunnel the
method further comprises the step of stripping, from
the received message, the tunnel receiving endpoint ad-
5 dress, before forwarding the message through the tunnel
receiving endpoint port.

17. Apparatus for logically connecting local
area networks (LANs) interconnected by network compo-
nents that include bridges and may include routers, the
apparatus comprising:

5 a plurality of bridges with the capability to
form tunnels between LANs that may be widely separated,
such bridges being referred to as tunnelers;

means contained collectively within the tunnel-
ers, for electing a unique designated tunneler for each
10 extended LAN (XLAN) for which tunneling is to be provid-
ed, wherein each XLAN has no more than one designated
tunnelers, but a single tunnelers may be designated by
more than one XLAN;

means for configuring the tunnelers by supply-
15 ing each with information identifying other tunnelers
with which a tunnel may be established;

means contained collectively in at least two
tunnelers, for establishing at least one tunnel between
two of the tunnelers, by exchanging messages between
20 the two tunnelers; and

means contained within each tunnelers, for se-
lectively forwarding message traffic through the estab-
lished tunnel, from one LAN to another.

18. Apparatus as defined in claim 17, wherein the means for electing a unique designated tunneler for each XLAN includes:

means for executing a spanning tree algorithm
5 among all of the bridges connected to the XLAN, and thereby electing a root bridge; and

means for ensuring that the root bridge has tunneling capability.

19. Apparatus as defined in claim 17, wherein the means for configuring the tunnelers includes:

means for supplying to each tunneler the identities of other tunnelers and the identities of ports
5 through which the other tunnelers are connected to XLANs with which they are associated.

20. Apparatus as defined in claim 19, wherein the means for establishing at least one tunnel includes:

means for transmitting a greeting from a designated tunneler to each other tunneler that is a potential tunnel endpoint;
5

means for receiving a message from one of the potential tunnel endpoints confirming that a tunnel may be established; and

10 means for recording that a tunnel has been established.

21. Apparatus as defined in claim 17, wherein the means for configuring the tunnelers includes:

means for supplying to each tunneler the identities of other tunnelers, the identities of ports
5 through which the other tunnelers are connected to XLANs with which they are associated, and an indication of tunneler priorities, to facilitate establishment of tunnels between tunnel endpoints.

22. Apparatus as defined in claim 20, wherein the means for establishing at least one tunnel includes:

5 means for transmitting a greeting from a designated tunneler to another designated tunneler that is a potential tunnel endpoint;

means for receiving a message from the other designated tunneler confirming that a tunnel may be established; and

10 means for recording that a tunnel has been established.

23. Apparatus as defined in claim 20, wherein the means for establishing at least one tunnel includes:

5 means for transmitting a greeting from a designated tunneler to another designated tunneler that is a potential tunnel endpoint;

means for transmitting, after failing to receive a confirming message from the other designated tunneler, a greeting to at least one backup tunneler;

10 means for receiving a message from the backup tunneler confirming that a tunnel may be established; and

means for recording that a tunnel has been established.

24. Apparatus as defined in claim 17, wherein the means for selectively forwarding message traffic through the established tunnel includes:

means for receiving a message at a tunneler;

5 means for determining whether the message destination is known to the tunneler;

means operative if the destination is known,
for
determining whether the destination re-
quires forwarding through a tunnel, and
if so, forwarding the message through the
tunnel, if the tunnel has been established and
the message is of a type authorized for for-
warding through the tunnel;
means operative if the destination is not
known, for determining whether the message was received
from a tunnel;
means operative if the message was received
from a tunnel, for forwarding the message through a
port defined as the tunnel endpoint;
means operative if the message was not re-
ceived from a tunnel and the message destination is not
known, for
forwarding the message over all permissi-
ble non-tunnel ports, and
forwarding the message through all estab-
lished tunnels, if any, for which this tunnel-
er is a sending endpoint, if the message is of a
type authorized for tunnel transmission.

25. Apparatus as defined in claim 24, wherein
the means for forwarding a message through a tunnel in-
cludes:

means for appending to the message a destina-
tion address that includes the address of a receiving
endpoint tunneler of the tunnel, and also includes a
port identifier that defines, in part, the receiving
endpoint of the tunnel; and
means for transmitting the message through an
appropriate port to reach the receiving endpoint of the
tunnel.

26. Apparatus as defined in claim 25, and further comprising :

means operative if the message was received from a tunnel, for stripping from the received message the tunnel receiving endpoint address, before forwarding the message through the tunnel receiving endpoint port.

27. Apparatus as defined in claim 17, wherein:

the means for configuring includes means for supplying the tunnelers with a subset of information concerning other tunnelers, the subset of information being optimized for a particular network topology; and

the means for establishing a tunnel includes

(1) for a designated tunneler, means for sending a greeting to another designated tunneler with which it has been configured, and receiving a response confirming that a tunnel has been established,

(2) for a designated tunneler, means for sending a greeting to a nondesignated tunneler with which it has been configured, means for receiving a refusal response identifying a designated tunneler, means for redirecting the greeting to the designated tunneler identified in the refusal response, and receiving a response confirming that a tunnel has been established, and

25 (3) for a nondesignated tunneler, means
for periodically transmitting multicast messages identifying the tunnelers with which it has
been configured, and, for a designated tunnel-
er, means for responding to a multicast mes-
30 sage from a nondesignated tunneler, by sending
a greeting to one of the tunnelers contained
in the multicast message, and receiving a re-
sponse message confirming that a tunnel has
30 been established.

28. A method for logically connecting local area
network substantially as described with reference to the
accompanying drawings.

29. Apparatus for logically connecting local area
networks substantially as described with reference to the
accompanying drawings.

1/3

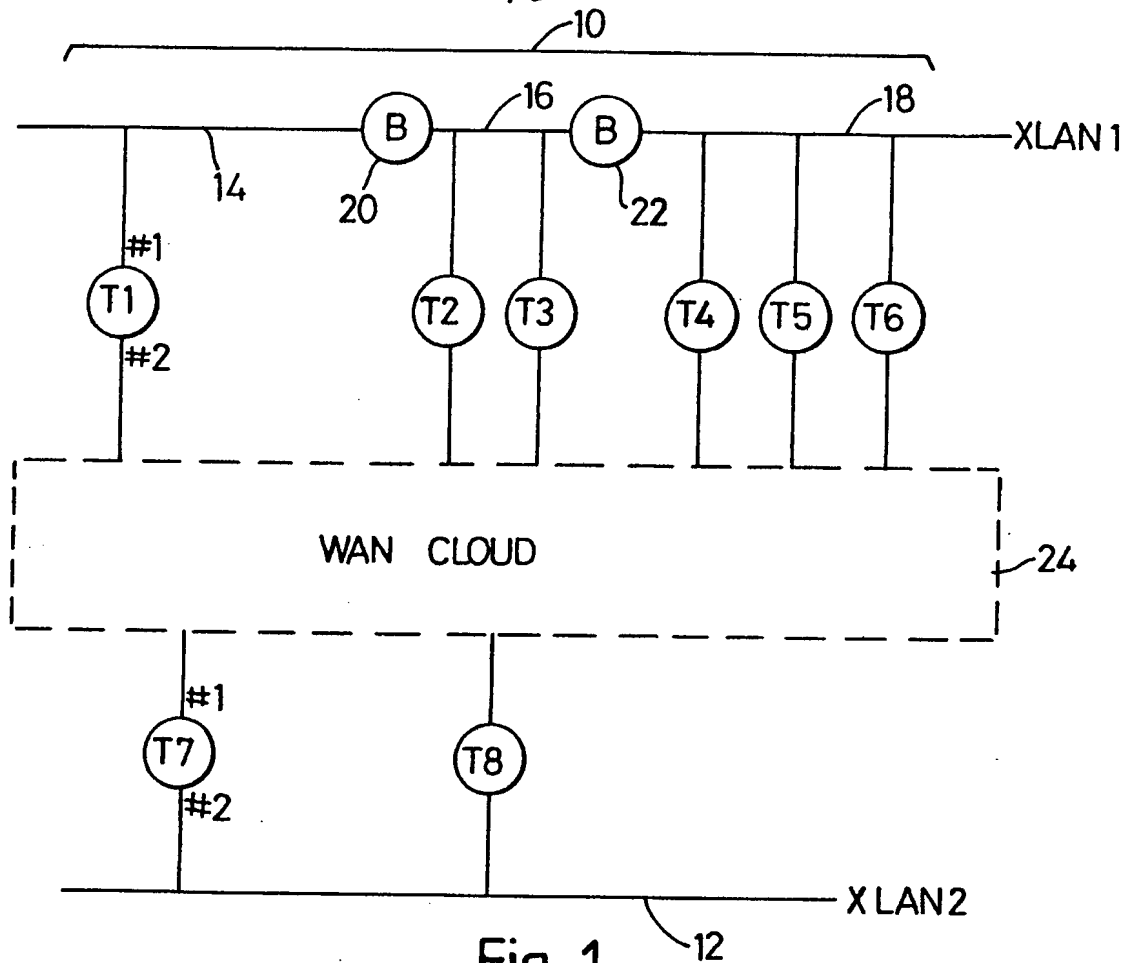


Fig. 1

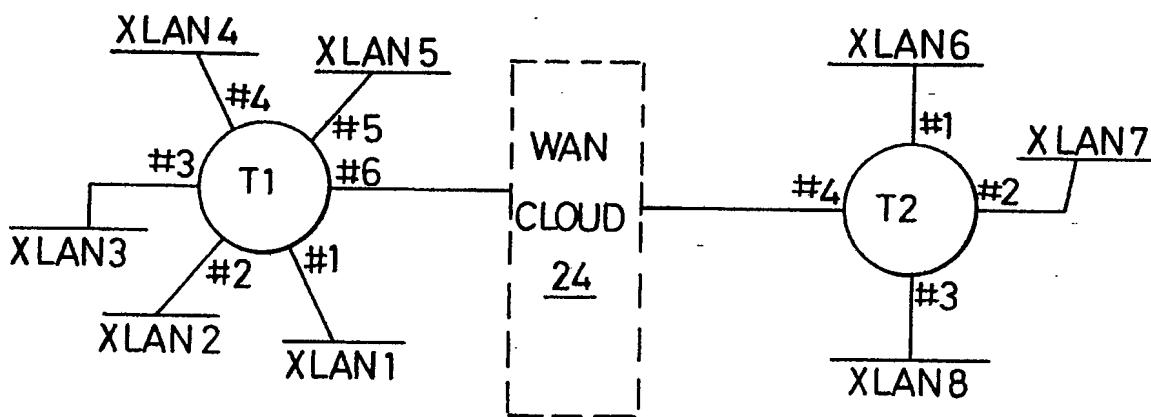
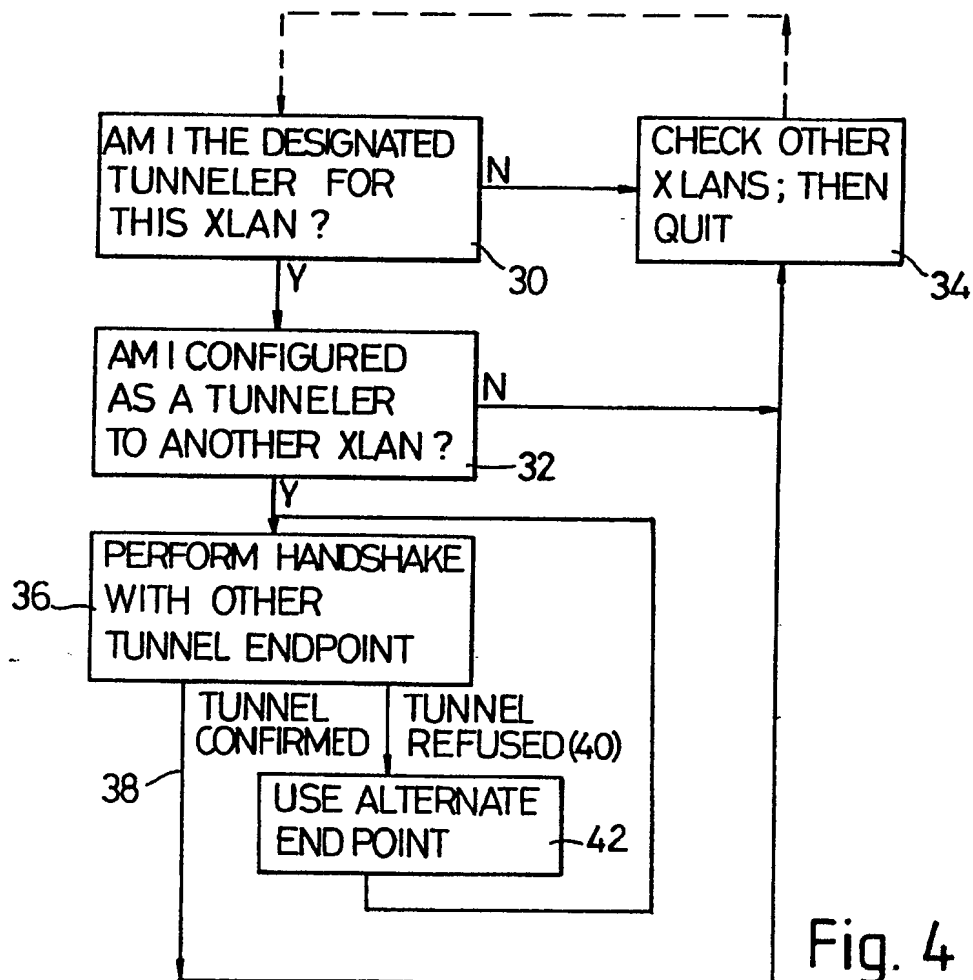
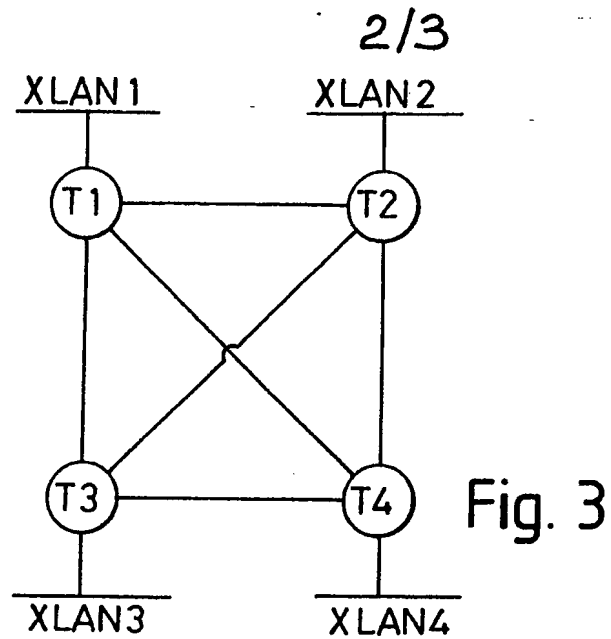


Fig. 2



3/3

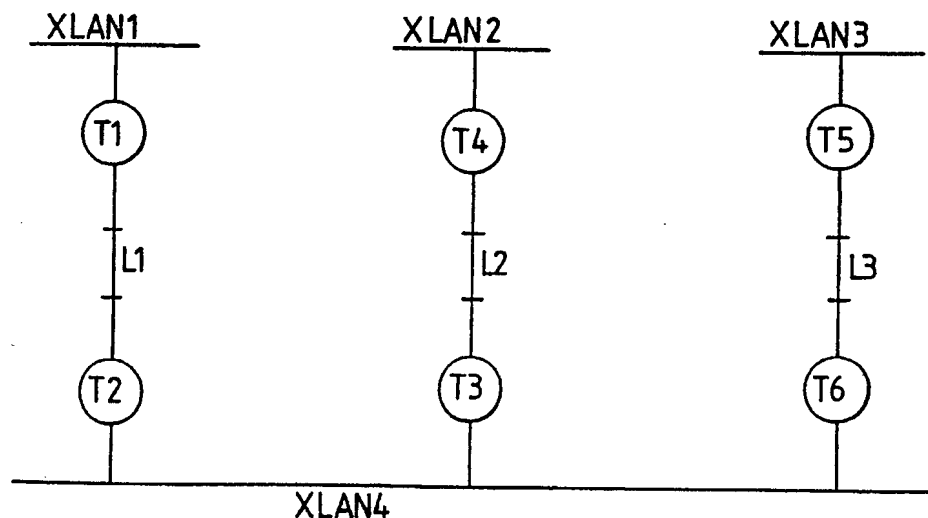
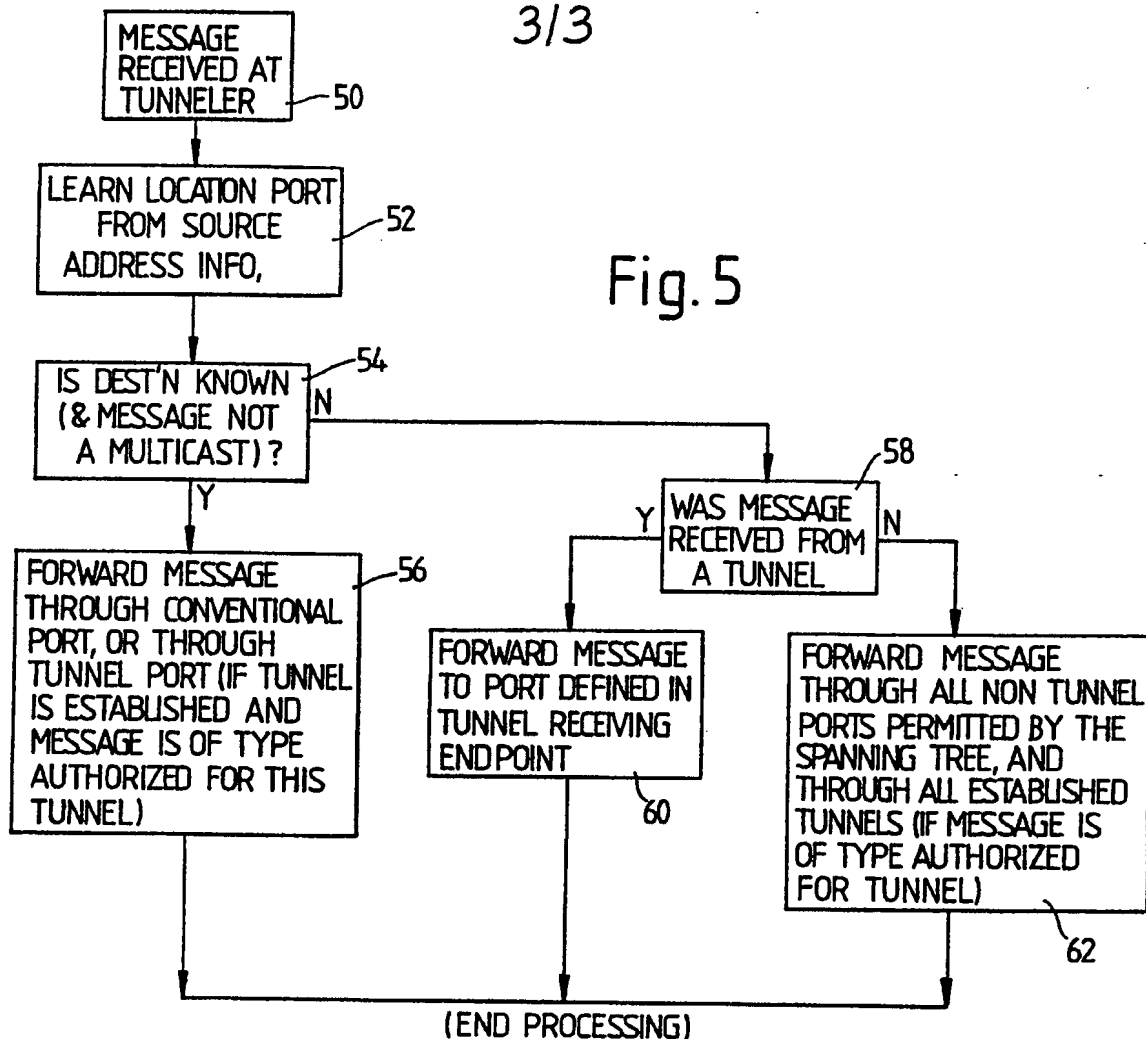
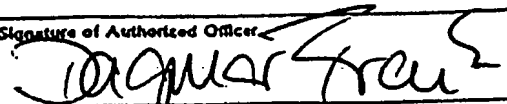


Fig. 6

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/GB 92/00034

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all) *		
According to International Patent Classification (IPC) or to both National Classification and IPC		
IPC ⁵ : H 04 L 12/46, G 06 F 13/00, G 06 F 15/16		
II. FIELDS SEARCHED		
Minimum Documentation Searched *		
Classification System	Classification Symbols	
IPC ⁵	H 04 L, G 06 F, H 04 J	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched *		
III. DOCUMENTS CONSIDERED TO BE RELEVANT*		
Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages **	Relevant to Claim No. **
A	WO, A1, 90/16 026 (HALLEY SYSTEMS) 27 December 1990 (27.12.90), see abstract; page 2, line 31 - page 4, line 30; fig. 1.	1, 13, 17
A	EP, A2, 0 222 584 (UNIVERSITY OF SALFORD) 20 May 1987 (20.05.87), see abstract; column 1, lines 3-15; column 3, lines 19-33.	1, 13, 17
A	EP, A2, 0 324 277 (VITALINK) 19 July 1989 (19.07.89), see abstract; page 4, lines 15-20.	1, 2, 13, 17
A	EP, A2, 0 374 883 (FUJITSU) 27 June 1990 (27.06.90), see abstract; column 2, lines	1, 13, 17
<p>* Special categories of cited documents: **</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another claim or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"Z" document member of the same patent family</p>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report	
02 April 1992	24.04.92	
International Searching Authority	Signature of Authorized Officer	
EUROPEAN PATENT OFFICE		

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)		
Category *	Citation of Document, " with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	<p>9-36; fig. 1,2. --</p> <p>US, A, 4 922 503 (LEONE) 01 May 1990 (01.05.90), see abstract; column 1, lines 5-20.</p>	1,13, 17
A	<p>--</p> <p>US, A, 4 897 841 (GANG Jr.) 30 January 1990 (30.01.90), see column 2, lines 19-44; fig. 1. -----</p>	1,13, 17

ANHANG

zum internationalen Recherchen-
bericht über die internationale
Patentanmeldung Nr.

ANNEX

to the International Search
Report to the International Patent
Application No.

ANNEXE

au rapport de recherche inter-
national relatif à la demande de brevet
international n°

PCT/GB92/00034 SAE 55161

In diesem Anhang sind die Mitglieder
der Patentfamilien der im obenge-
nannten internationalen Recherchenbericht
angeführten Patentedokumente angegeben.
Diese Angaben dienen nur zur Unter-
richtung und erfolgen ohne Gewähr.

This Annex lists the patent family
members relating to the patent documents
cited in the above-mentioned inter-
national search report. The Office is
in no way liable for these particulars
which are given merely for the purpose
of information.

La présente annexe indique les
membres de la famille de brevets
relatifs aux documents de brevets cités
dans le rapport de recherche inter-
national visé ci-dessus. Les renseigne-
ments fournis sont donnés à titre indica-
tif et n'engagent pas la responsabilité
de l'Office.

Im Recherchenbericht angeführtes Patentedokument Patent document cited in search report Document de brevet cité dans le rapport de recherche		Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
EP A2	374883	27-06-90	AU A1 46753/89	28-06-90
			AU B2 611068	30-05-91
			CA A 2005979	20-06-90
			EP A3 374883	06-11-91
			JP A2 2270437	05-11-90
EP A2	222584	20-05-87	EP A3 222584	19-07-89
			GB A0 8601820	26-02-86
			GB A0 8600645	19-02-86
			GB A0 8527582	11-12-85
EP A2	324277	19-07-89	AU A1 28303/89	20-07-89
			AU B2 607571	07-03-91
			DK A0 7335/88	30-12-88
			DK A 7335/88	16-07-89
			EP A3 324277	26-06-91
			IL A0 88799	31-07-89
			JP A2 2005647	10-01-90
			NO A0 885521	13-12-88
			NO A 885521	17-07-89
			US A 4811337	07-03-89
WD A1	9016026	27-12-90	AU A1 59516/90	08-01-91
US A	4922503	01-05-90	keine - none - rien	
US A	4897841	30-01-90	keine - none - rien	